

信息安全 安全可靠应用系统分类

Information security-classification for secure and reliable application system

2016 - 12 - 30 发布

2017 - 01 - 31 实施

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 应用系统模型	2
4.1 特征维	2
4.2 应用系统	2
5 安全可靠应用系统模型	2
5.1 属性	2
5.2 等级保护	3
5.3 应用系统	3
6 分类原则	3
6.1 系统性	3
6.2 可靠性	3
6.3 可信性	3
6.4 可用性	3
7 分类主题	3
7.1 综述	3
7.2 领域应用	3
7.3 网络行为	4
8 类型	4
8.1 领域应用	4
8.2 网络应用	5
附录 A (规范性附录) 应用系统模型	7
附录 B (规范性附录) 安全可靠应用系统模型	8

前 言

本标准按照 GB/T1.1—2009《标准化工作导则 第1部分：标准的结构与编写》给出的规则起草。
本标准大连市经济和信息化委员会提出并归口。

本标准主要起草单位：大连软件行业协会、大连交通大学、大连市计算机学会、大连市经济和信息化委员会信息安全处。

本标准主要起草人：郎庆斌、尹宏、董晶、丁宗安、杨万清、杨莉、司丹、孙毅、王小庚、牟楠。

信息安全 安全可靠应用系统分类

1 范围

本标准定义了应用系统模型、安全可靠应用系统模型，规定了安全可靠应用系统的分类原则、分类主题和类型的基本规则。

本标准适用于各类应用系统的安全分类。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T22239-2008 信息系统安全保护基本要求

GB/T22240-2008 信息系统安全保护等级定级指南

（信安字[2007]10）信息系统安全等级保护实施指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全可靠 secure and reliable

在可预期和掌握的目标范围内，自有、自主实现预定功能，免受不可接受的损害风险。

3.2

自有 own

拥有权利，但仍受某些条件、因素的制约。

3.3

自有知识产权 own intellectual property

应用系统中，独立创造完成的非核心、关键技术，并依法履行了知识产权法定程序，受知识产权相关法律保护，但核心、关键技术不可控。

3.4

自主 independent

拥有权利，不受其它因素制约。

3.5

自主知识产权 independent intellectual property

应用系统中，独立创造完成的核心、关键技术，并依法履行了知识产权法定程序，受知识产权相关法律保护，且不受其它相关知识产权制约。

3.6

应用系统 **application system**

利用各种 IT 基础设备、应用平台解决各种实际问题的应用软件。

4 应用系统模型

4.1 特征维

应用系统可依据特征划分为2维：

a) 应用领域：应用系统所涉及的社会、经济、生活各个领域，更多体现的是目的特征，如：

- 1) 政务应用：办公自动化、政务/业务/商务处理、数据报表、统计分析、辅助决策等；
- 2) 计算机辅助设计、制造、测试：工程/产品设计、产品制造、产品/性能测试等；
- 3) 经济管理：经济信息管理、物资、财务、劳资等管理等；
- 4) 人力资源管理：人事管理等；
- 5) 金融应用：银行、证券、保险、信托等；
- 6) 自动控制：工控系统、智能控制、各类控制系统等；
- 7) 事务管理：各类管理信息系统等；
- 8) 教育应用：教育管理、教学应用等；
- 9) 医疗卫生：医疗管理、卫生健康等；
- 10) 军事应用；
- 11) ……………

b) 网络行为：网络应用的社会化特征，更多体现行为的因素。因而，基于网络的应用系统应根据网络行为分类。根据《中国互联网络发展状况统计报告》，网络空间行为可划分为5类：

- 1) 基础应用类：包括即时通信、搜索引擎、网络新闻、社交应用等；
- 2) 商务交易类：包括网络购物、网上外卖、团购等；
- 3) 网络金融类：包括互联网理财、网上支付等；
- 4) 网络娱乐类：包括网络游戏、网络文学、网络视频、网络音乐等；
- 5) 公共服务类：包括在线教育、在线政务、网约车等。

4.2 应用系统

应用系统的应用场景可以是多样的，如：

- a) 基于各种网络行为的应用，如电子政务、电子商务等；
- b) 独立运行的应用：
 - 1) 封闭在局域网内的应用，如工控系统等；
 - 2) 计算机系统的独立应用等。

应用系统模型，参看附录A。

5 安全可靠应用系统模型

5.1 属性

安全可靠应用系统的属性，可包括：

- a) 引进：应用系统的核心或关键部分完全采用不可控技术、方法等，无自有、自主知识产权；
- b) 部分自主：应用系统的核心部分完全采用不可控技术、方法等，部分关键或非关键技术具有自主知识产权；
- c) 自主安全可控：应用系统的核心和关键部分具有完全的自主知识产权，安全可控。

5.2 等级保护

依据GB/T22239、GB/T22240等国家信息安全等级保护相关标准系列，结合应用系统的属性，确定应用系统安全等级。

5.3 应用系统

依据应用系统模型，安全可靠应用系统应包括基于应用领域和基于网络行为2个分支。
安全可靠应用系统模型，参看附录B。

6 分类原则

6.1 系统性

应系统、整体评估应用系统的架构、功能，识别系统核心、关键技术属性。

6.2 可靠性

应评估分系统和系统整体的健壮性、稳定性，识别影响系统可靠性的因素，确定系统成熟度。

6.3 可信性

应评估应用系统的设计质量、过程质量和应用安全，识别应用系统质量保障体系的科学性、规范性。

6.4 可用性

应评估系统易用性、可维护性、可移植性和应用效能，识别应用系统应用领域、应用场景和资源适应的能力。

7 分类主题

7.1 综述

根据应用系统应用目标的发展和演变及科学、技术、社会应用的发展，并前瞻未来应用的发展，将安全可靠应用系统的分类主题定义为领域应用和网络行为2大类。

7.2 领域应用

按领域应用定义的安全可靠应用系统的分类主题，主要应包括：

- a) 核心技术：可依据应用系统的属性确定应用系统类别和等级；
- b) 自有产权：部分核心或关键技术、或部分非关键技术具有自主知识产权，可达到部分可控，但系统不具有独立性，并可依此确定类别和等级；
- c) 自主产权：核心或关键技术具有自主知识产权，系统独立、可控，并可依此确定类别和等级；

- d) 成熟度：应用系统的开发模式、应用模式、技术能力、应用环境等相对先进、成熟，系统产品经过市场测试、检验，并可依此评估系统可靠性、可用性、稳定性，确定类别和等级；
- e) 应用领域：可依据应用领域的安全等级、应用风险等评估、确定类别和等级；
- f) 关键价值：可根据应用场景、关键业务的价值评估、确定类别和等级。

7.3 网络行为

按网络行为定义的安全可靠应用系统的分类主题，亦适用7.2，同时应包括：

- a) 关键价值：可根据网络行为、应用场景、关键业务的价值评估、确定类别和等级；
- b) 应用行为：可根据网络应用行为的可信性，评估、确定类别和等级；
- c) 隐私安全：应考虑并评估隐私相关程度和价值及相应的安全威胁等级，确定类别和等级；
- d) 资源裕度：应评估系统应用涉及的资源丰裕度、相关资源价值、资源风险等级等，确定类别和等级。

注：可信性：网络空间行为的可信性，包括基于网络环境的可信性、网络空间行为主体的可信性、网络空间内容可信性和网络空间行为可信性等。

8 类型

8.1 领域应用

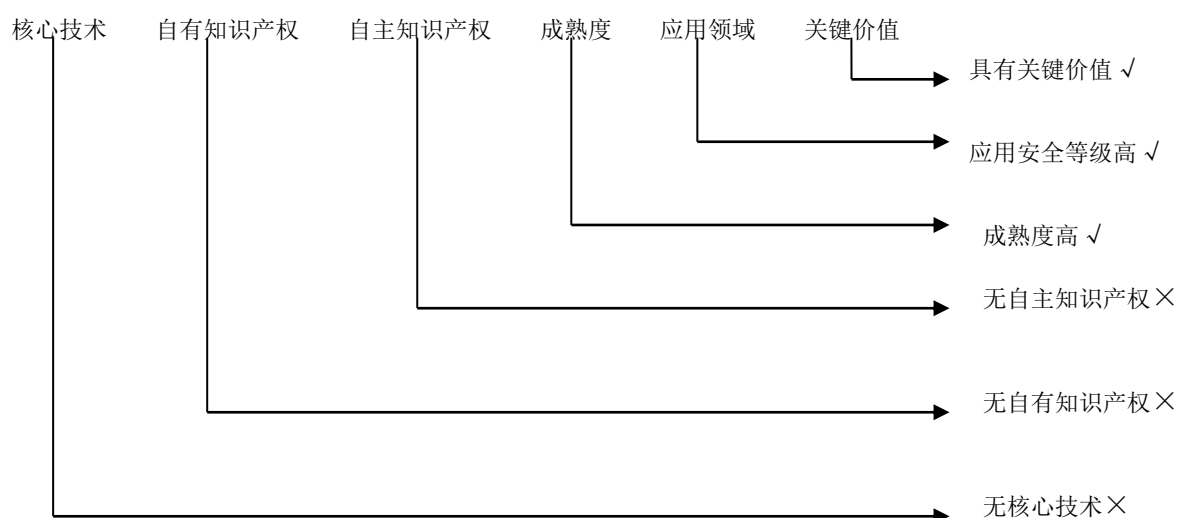
应依据领域应用的分类主题划分安全可靠应用系统类型：

- a) E类：应用于关键基础设施或关键领域，无自有、自主知识产权，系统不可控；
- b) D类：应用于非关键基础设施或非关键领域，无自有、自主知识产权，系统不可控；
- c) C类：应用于关键基础设施或关键领域，部分关键技术具有自有产权，系统核心部分不可控；
- d) B类：应用于非关键基础设施或非关键领域，部分关键技术具有自有产权，系统核心部分不可控；
- e) A类：应用于关键基础设施或关键领域，系统核心部分和关键技术具有完全自主产权，系统可控。

表1 领域应用分类

分类主题	类型				
	A	B	C	D	E
核心技术	√	×	×	×	×
自有知识产权	√	√	√	×	×
自主知识产权	√	×	×	×	×
成熟度	√	√	√	√	√
应用领域	√	×	√	×	√
关键价值	√	×	√	×	√

示例1：X 电力行业工控系统，采用 X 国际知名品牌产品：



该系统应为E类。

8.2 网络应用

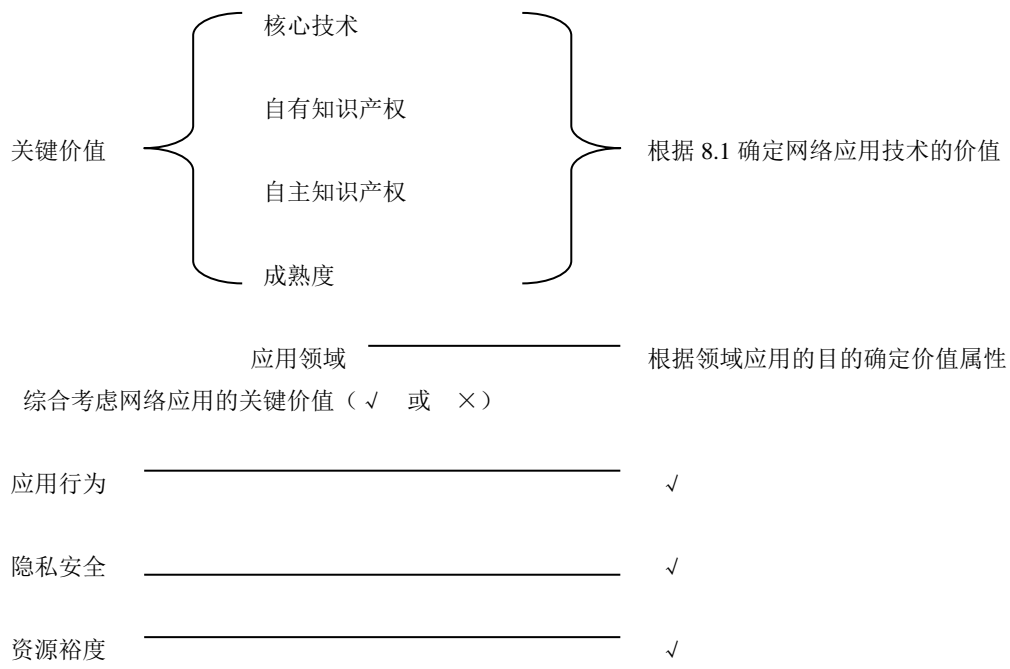
应依据网络行为评估基于网络的应用系统的安全性、可靠性，并依据分类主题划分类型：

- a) D类：无任何功利性目的、可满足听觉、视觉或知识、信息获取的一般性应用，应用行为单一，隐私度较低。如网络游戏、娱乐、新闻获取、电子书刊等；
- b) C类：利用网络空间特征，通过集群效应获取服务，隐私度较高。如网上聊天、电子邮件、短信、微信、微博、社区等；
- c) B类：通过网络实现传统公共服务的虚拟化，隐私度较高，资源裕度较高。如电子政务系统、网络教育、网络医院等；
- d) A类：通过网络实现金融、商务等交易服务的虚拟化，隐私度和资源裕度高。如网上金融服务、电子商务等。

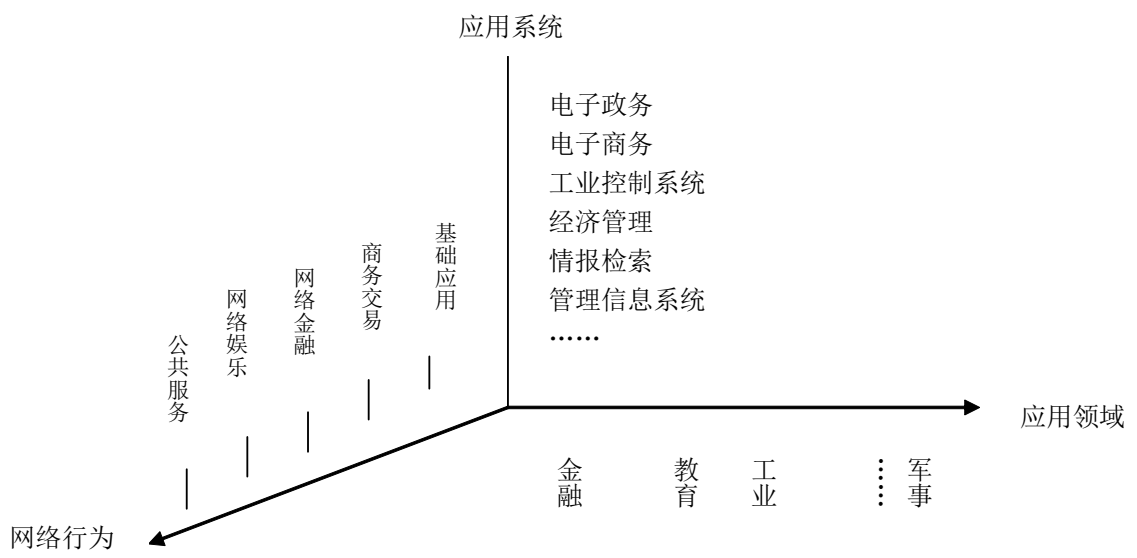
表2 网络行为分类

分类主题	类型			
	A	B	C	D
关键价值	✓	✓/×	×	×
应用行为	✓	✓	✓	×
隐私安全	✓	✓	✓	✓
资源裕度	✓	✓	×	×

示例2：智能应用（智能医疗、智能交通、智能……）



附录 A
(规范性附录)
应用系统模型



附录 B
(规范性附录)
安全可靠应用系统模型

